

Fields generated by torsion points of elliptic curves

Andrea Bandini¹ and Laura Paladino^{*2}

¹Dipartimento di Matematica e Informatica, Università degli Studi di Parma, Parco Area delle Scienze, 53/A - 43124 Parma, Italy, e-mail: andrea.bandini@unipr.it

²Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo, 5 - 56127 Pisa, Italy, e-mail: paladino@mail.dm.unipi.it

Keywords: elliptic curves; torsion points; Galois representations

Mathematics subject classification: 11G05; 11F80

Abstract

Let K be a field and let \mathcal{E} be an elliptic curve defined over K . Let m be a positive integer, prime with $\text{char}(K)$ if $\text{char}(K) \neq 0$; we denote by $\mathcal{E}[m]$ the m -torsion subgroup of \mathcal{E} and by $K_m := K(\mathcal{E}[m])$ the field obtained by adding to K the coordinates of the points of $\mathcal{E}[m]$. Let $P_i := (x_i, y_i)$ ($i = 1, 2$) be a \mathbb{Z} -basis for $\mathcal{E}[m]$; then $K_m = K(x_1, y_1, x_2, y_2)$. We look for small sets of generators for K_m inside $\{x_1, y_1, x_2, y_2, \zeta_m\}$ trying to emphasize the role of ζ_m (a primitive m -th root of unity). In particular, we prove that $K_m = K(x_1, \zeta_m, y_2)$, for any odd $m \geq 5$. When m is prime and K is a number field we prove that the generating set $\{x_1, \zeta_m, y_2\}$ is often minimal. We also describe explicit generators, degree and Galois groups of the extensions K_m/K for $m = 3$ and $m = 4$, when $\text{char}(K) \neq 2, 3$.

1 Introduction

Let K be a field of any characteristic and let \mathcal{E} be an elliptic curve defined over K . Let m be a positive integer, prime with $\text{char}(K)$ if $\text{char}(K) \neq 0$. We denote by $\mathcal{E}[m]$ the m -torsion subgroup of \mathcal{E} and by $K_m := K(\mathcal{E}[m])$ the field generated by the points of $\mathcal{E}[m]$, i.e. the field obtained by adding to K the coordinates of the m -torsion points of \mathcal{E} . As usual, for any point $P \in \mathcal{E}$, we let $x(P)$, $y(P)$ be its coordinates and we indicate its m -th multiple simply by mP . We denote by $\{P_1, P_2\}$ a \mathbb{Z} -basis for $\mathcal{E}[m]$; then $K_m = K(x(P_1), x(P_2), y(P_1), y(P_2))$. To ease notation, we put $x_i := x(P_i)$ and $y_i := y(P_i)$ ($i = 1, 2$). By Artin's primitive element theorem the extension K_m/K is monogeneous and one can find a unique generator for K_m/K by combining the above coordinates. On the other hand, by the properties of the Weil pairing e_m , we have that $e_m(P_1, P_2) \in K_m$ is a primitive m -th root of unity (we denote it by ζ_m). We want to emphasize the importance of ζ_m as a generator of K_m/K and look for minimal (i.e., with the smallest number of elements) sets of generators contained in $\{x_1, x_2, y_1, y_2, \zeta_m\}$. This kind of information is useful for describing the fields in terms of degrees and Galois groups, as we shall explicitly show for $m = 3$ and $m = 4$, when $\text{char}(K) \neq 2, 3$. Other

^{*}L. Paladino is partially supported by Istituto Nazionale di Alta Matematica, grant research *Assegno di ricerca Ing. G. Schirillo*, and partially supported by the European Commission and by Calabria Region through the European Social Fund.

applications are local-global problems (see, e.g., [5] or the particular cases of [10] and [11]), descent problems (see, e.g., [13] and the references there or, for a particular case, [2] and [3]), Galois representations, points on modular curves (see Section 4) and points on Shimura curves.

It is easy to prove that $K_m = K(x_1, x_2, \zeta_m, y_1)$ (see Lemma 2.1) and we expected a close similarity between the roles of the x -coordinates and y -coordinates; this turned out to be true in relevant cases. Indeed in Section 3 (mainly by analysing the possible elements of the Galois group $\text{Gal}(K_m/K)$) we prove that $K_m = K(x_1, \zeta_m, y_1, y_2)$ at least for odd $m \geq 5$. This leads to the following (for more precise and general statements see Theorems 2.8, 3.1 and 3.6)

Theorem 1.1. *If $m \geq 3$, then $K_m = K(x_1 + x_2, x_1 x_2, \zeta_m, y_1)$. Moreover if $m \geq 4$, then*

$$K_m = K(x_1, \zeta_m, y_1, y_2) \implies K_m = K(x_1, \zeta_m, y_2) .$$

In particular $K_m = K(x_1, \zeta_m, y_2)$ for any odd integer $m \geq 5$.

Note that, by Theorem 1.1, we have $K_p = K(x_1, \zeta_p, y_2)$, for any prime $p \geq 5$. The set $\{x_1, \zeta_p, y_2\}$ seems a good candidate (in general) for a minimal set of generators for K_p/K . Indeed, when K is a number field and \mathcal{E} has no complex multiplication, by Serre's open image theorem (see, e.g., [17, Appendix C, Theorem 19.1]), we expect that the natural representation

$$\rho_{\mathcal{E},p} : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

provides an isomorphism $\text{Gal}(K_p/K) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for almost all primes p , and there are hypotheses on x_1 , ζ_m and y_2 (see Theorem 4.3) which guarantee that

$$[K(x_1, \zeta_m, y_2) : K] = (p^2 - 1)(p^2 - p) = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})| .$$

For (almost all) the *exceptional primes* for which $|\text{Gal}(K_p/K)| < |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})|$ (see Definition 4.5), we employ some well known results on Galois representations and on subgroups of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to reduce further the set of generators. Joining the results of Lemma 4.7, Theorem 4.9 and Theorem 4.10 we obtain

Theorem 1.2. *Let K be a number field. Assume that $p \geq 53$ is unramified in K/\mathbb{Q} and exceptional for the curve \mathcal{E} . Then*

1. $p \equiv 2 \pmod{3} \implies K_p = K(\zeta_p, y_2);$
2. $p \equiv 1 \pmod{3} \implies [K_p : K(\zeta_p, y_2)]$ is 1 or 3.

In Subsection 4.3 we give just a hint of the possible applications to points of modular curves. Similar applications, even to Shimura curves, can be further developed in the future. Modular curves might provide a different approach (and more insight) to problems analogous to those treated here.

The final sections are dedicated to the cases $m = 3$ and $m = 4$, when $\text{char}(K) \neq 2, 3$. We use the explicit formulas for the coordinates of the torsion points to give more information on the extensions K_3/K and K_4/K , such as their degrees and their Galois groups.

Acknowledgement. The authors would like to express their gratitude to Antonella Perucca for suggesting the topic of a generalization of the results of [4] and for providing several suggestions, comments and improvements on earlier drafts of this paper.

2 The equality $K_m = K(x_1 + x_2, x_1x_2, \zeta_m, y_1)$

As mentioned above, we consider a field K of any characteristic and an elliptic curve \mathcal{E} defined over K . Throughout the paper we always assume that m is an integer, $m \geq 2$ and, if $\text{char}(K) \neq 0$, that m is prime with $\text{char}(K)$. We choose two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ which form a \mathbb{Z} -basis of the m -torsion subgroup $\mathcal{E}[m]$ of \mathcal{E} . We define $K_m := K(\mathcal{E}[m])$ and we denote by $K_{m,x}$ the extension of K generated by the x -coordinates of the points in $\mathcal{E}[m]$. So we have

$$K(x_1, x_2) \subseteq K_{m,x} \subseteq K_m = K(x_1, x_2, y_1, y_2) .$$

Let $e_m : \mathcal{E}[m] \times \mathcal{E}[m] \rightarrow \mu_m$ be the Weil Pairing, where μ_m is the group of m -th roots of unity. By the properties of e_m , we know that $\mu_m \subset K_m$ and, once P_1 and P_2 are fixed, we put $e_m(P_1, P_2) =: \zeta_m$ (a primitive m -root of unity). We remark that the choice of P_1 and P_2 is arbitrary; we use this convention for ζ_m (which obviously has no effect on the generated field since $K(\zeta_m) = K(\mu_m)$ for any primitive m -th root of unity) to simplify notations and computations. In particular for any $\sigma \in \text{Gal}(K_m/K)$, we have

$$\sigma(\zeta_m) = \sigma(e_m(P_1, P_2)) = e_m(P_1^\sigma, P_2^\sigma) = \zeta_m^{\det(\sigma)},$$

where, for simplicity, we still use σ to denote the matrix $\rho_{\mathcal{E},m}(\sigma) \in \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

The next lemma is rather obvious, but it shows how ζ_m can play the role of one of the y -coordinates in generating K_m and it will be useful in the rest of the paper.

Lemma 2.1. *We have $K_m = K(x_1, x_2, \zeta_m, y_1)$.*

Proof. An endomorphism of $\mathcal{E}[m]$ fixing P_1 and x_2 is of type $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. If it also fixes ζ_m , then $\det(\sigma) = 1$ and eventually $\sigma = \text{Id}$. \square

We now show that ζ_m and y_1y_2 are closely related over the field $K(x_1, x_2)$. Let (x_3, y_3) (resp. (x_4, y_4)) be the coordinates of the point $P_3 := P_1 + P_2$ (resp. $P_4 := P_1 - P_2$). By the group law of \mathcal{E} , we may express x_3 and x_4 in terms of x_1, x_2, y_1 and y_2 :

$$x_3 = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2 \quad \text{and} \quad x_4 = \frac{(y_1 + y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2 \quad (1)$$

(note that $x_1 \neq x_2$ because P_1 and P_2 are independent). By taking the difference of these two equations we get

$$y_1y_2 = \frac{(x_4 - x_3)(x_1 - x_2)^2}{4} . \quad (2)$$

Lemma 2.2. *We have $K(x_1, x_2, y_1y_2) = K(x_1, x_2, x_3, x_4)$ and $K_m = K_{m,x}(y_1)$*

Proof. Since $y_i^2 \in K(x_i)$, equations (1) and (2) prove the first equality. For the final statement just note that $K_m = K_{m,x}(y_1, y_2) = K_{m,x}(y_1)$. \square

More precisely, we have

Lemma 2.3. *Let $L = K(x_1, x_2)$. Exactly one of the following cases holds:*

1. $[K_m : L] = 1$;
2. $[K_m : L] = 2$ and $L(y_1y_2) = K_m$;

3. $[K_m : L] = 2$, $L = L(y_1 y_2)$ and $L(y_1) = L(y_2) = K_m$;

4. $[K_m : L] = 4$ and $[L(y_1 y_2) : L] = 2$.

Proof. Obviously the degree of K_m over L divides 4. If $[K_m : L] = 1$, then we are in case **1**. If $[K_m : L] = 4$, then y_1 and y_2 must generate different quadratic extensions of L and so $[L(y_1 y_2) : L] = 2$ and we are in case **4**. If $[K_m : L] = 2$ and $y_1 y_2 \notin L$, then we are in case **2**. Now suppose that $[K_m : L] = 2$ and $y_1 y_2 \in L$. Then y_1 and y_2 generate the same extension of L and this extension is nontrivial, so we are in case **3**. \square

Lemma 2.4. *If $y_1 y_2 \notin K(x_1, x_2)$, then $\zeta_m \notin K(x_1, x_2)$.*

Proof. We are in case **2** or case **4** of Lemma 2.3 and, in particular, $m > 2$ because of $K_2 = L$. We have $[L(y_1 y_2) : L] = 2$ and there exists $\tau \in \text{Gal}(K_m/L)$ such that $\tau(y_1 y_2) = -y_1 y_2$. Without loss of generality, we may suppose $\tau(y_1) = -y_1$ and $\tau(y_2) = y_2$ so that $\tau = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\tau(\zeta_m) = \zeta_m^{-1}$. Since $m \neq 2$, $\zeta_m^{-1} \neq \zeta_m$ and we get $\zeta_m \notin L$. \square

The connection between ζ_m and $y_1 y_2$ is provided by the following statement.

Theorem 2.5. *We have*

$$K(x_1, x_2, \zeta_m) = K(x_1, x_2, y_1 y_2) .$$

Proof. We first prove that $\zeta_m \in K(x_1, x_2, y_1 y_2)$ by considering the four cases of Lemma 2.3.

Case 1 or 2: we have $K(x_1, x_2, y_1 y_2) = K_m$ so the statement clearly holds.

Case 3: we have $K_m = L(y_1)$ and $y_1 y_2 \in L$ so the nontrivial element $\tau \in \text{Gal}(K_m/L)$ maps y_i to $-y_i$ for $i = 1, 2$. In particular, $\tau = -\text{Id}$ and $\tau(\zeta_m) = \zeta_m$. Hence $\zeta_m \in L = K(x_1, x_2)$.

Case 4: since $K_m = L(y_1, y_2)$ and $\text{Gal}(K_m/L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, there exists $\tau \in \text{Gal}(K_m/L)$ such that $\tau(y_i) = -y_i$ for $i = 1, 2$. The field fixed by τ is $L(y_1 y_2)$ and, as in the previous case, we get $\tau(\zeta_m) = \zeta_m$ so $\zeta_m \in L(y_1 y_2) = K(x_1, x_2, y_1 y_2)$.

Now the statement of the theorem is clear if we are in case **1** or in case **3** of Lemma 2.3. In cases **2** and **4** of Lemma 2.3 we have $[L(y_1 y_2) : L] = 2$, $\zeta_m \notin L$ (Lemma 2.4) and $L(\zeta_m) \subseteq L(y_1 y_2)$. These three facts yield $L(\zeta_m) = L(y_1 y_2)$. \square

We conclude this section with the equality appearing in the title, which still focuses more on the x -coordinates. For that we shall need the following lemma.

Lemma 2.6. *The extension $K(x_1, x_2)/K(x_1 + x_2, x_1 x_2)$ has degree ≤ 2 . Its Galois group is either trivial or generated by σ with $\sigma(x_i) = x_j$ ($i \neq j$).*

Proof. Just note that x_1 and x_2 are the roots of $X^2 - (x_1 + x_2)X + x_1 x_2$. \square

Corollary 2.7. *We have $K(\zeta_m + \zeta_m^{-1}) \subseteq K(x_1 + x_2, x_1 x_2)$.*

Proof. This is obvious if $K(x_1, x_2) = K(x_1 + x_2, x_1 x_2)$. If they are different, take the nontrivial element σ of $\text{Gal}(K(x_1, x_2)/K(x_1 + x_2, x_1 x_2))$. By Lemma 2.6, we have $\sigma(P_i) = \pm P_j$ ($i \neq j$), hence $\det(\sigma) = \pm 1$. \square

Theorem 2.8. *For $m \geq 3$ we have $K_m = K(x_1 + x_2, x_1 x_2, \zeta_m, y_1)$.*

Proof. We consider the tower of fields

$$K(x_1 + x_2, x_1x_2) \subseteq K(x_1, x_2) \subseteq K(x_1, x_2, \zeta_m, y_1) = K_m$$

and adopt the following notations:

$$\begin{aligned} G &:= \text{Gal}(K_m/K(x_1 + x_2, x_1x_2)) , \\ H &:= \text{Gal}(K_m/K(x_1, x_2)) \triangleleft G , \\ G/H &= \text{Gal}(K(x_1, x_2)/K(x_1 + x_2, x_1x_2)) . \end{aligned}$$

If $K(x_1 + x_2, x_1x_2) = K(x_1, x_2)$, then the statement holds by Lemma 2.1.

By Lemma 2.6, we may now assume that G/H has order 2 and its nontrivial automorphism swaps x_1 and x_2 . Then there is at least one element $\tau \in G$ such that $\tau(x_i) = x_j$, with $i, j \in \{1, 2\}$ and $i \neq j$. Therefore $\tau(y_i) = \pm y_j$. The possibilities are:

$$\tau = \pm\tau_1 = \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix} \text{ (of order 2) and } \tau = \pm\tau_2 = \begin{pmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{pmatrix} \text{ (of order 4) .}$$

Note that $\tau_2^2 = -\text{Id}$ fixes both x_1 and x_2 , i.e. the generators of the field L of Lemma 2.3. Moreover, if $y_2 = \pm y_1$, then we have

$$\tau_2^2(P_1) = \tau_2(P_2) = \tau_2(x_2, \pm y_1) = (x_1, \pm y_2) = P_1,$$

a contradiction. The automorphisms τ_1 and τ_2 generate a non abelian group of order 8 with two elements of order 4, i.e., the dihedral group

$$D_4 = \langle \tau_1, \tau_2 : \tau_1^2 = \tau_2^4 = \text{Id} \text{ and } \tau_1\tau_2\tau_1 = \tau_2^3 \rangle .$$

So G is a subgroup of D_4 . Since G/H has order 2, H is isomorphic to either 1, $\mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$ (note that $\tau_2 \notin H$) and its nontrivial elements can at most be the following

$$\tau_1\tau_2 = \tau_2^3\tau_1 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} , \tau_2\tau_1 = \tau_1\tau_2^3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } -\text{Id} .$$

We distinguish three cases according to the possible degrees $[K_m : K(x_1, x_2)]$ mentioned in Lemma 2.3.

The case $K_m = K(x_1, x_2)$. Since $|H| = 1$ and $|G/H| = 2$, then $|G| = 2$. The nontrivial automorphism of G has to be $\pm\tau_1$. In both cases G does not fix ζ_m : so $\zeta_m \in K(x_1, x_2) - K(x_1 + x_2, x_1x_2)$ and we deduce $K(x_1 + x_2, x_1x_2, \zeta_m) = K(x_1, x_2) = K_m$.

The case $[K_m : K(x_1, x_2)] = 4$. Since $|H| = 4$ and $|G/H| = 2$, we have $G \simeq D_4$. The subgroup $\langle \tau_2 \rangle$ of D_4 is normal of index 2 and it does not contain τ_1 . Moreover, τ_2 fixes ζ_m and τ_1 does not. Then we have

$$\text{Gal}(K_m/K(x_1 + x_2, x_1x_2, \zeta_m)) = \langle \tau_2 \rangle$$

and $[K(x_1 + x_2, x_1x_2, \zeta_m) : K(x_1 + x_2, x_1x_2)] = 2$. If $y_1^2 \in K(x_1 + x_2, x_1x_2, \zeta_m)$, then $y_1^2 = \tau_2(y_1)^2 = y_2^2$, giving $y_1 = \pm y_2$ and we already ruled this out. Then the degree of the extensions

$$K(x_1 + x_2, x_1x_2) \subset K(x_1 + x_2, x_1x_2, \zeta_m) \subset K(x_1 + x_2, x_1x_2, \zeta_m, y_1)$$

are, respectively, 2 and at least 4. Since the extension $K_m/K(x_1 + x_2, x_1x_2)$ has degree 8 the statement follows.

The case $[K_m : K(x_1, x_2)] = 2$. Since $|H| = 2$ and $|G/H| = 2$, then $|G| = 4$. We have to exclude $G = \langle \tau_2 \tau_1, -\text{Id} \rangle$, because these automorphisms fix both x_1 and x_2 , so we would have $G = H$. We are left with $H = \langle -\text{Id} \rangle$ and one the following two possibilities:

$$G = \langle \tau_2 \rangle \quad \text{or} \quad G = \langle \tau_1, -\text{Id} \rangle .$$

We now consider each of the two subcases separately. Assume $G = \langle \tau_2 \rangle$ and recall that $y_1 \neq \pm y_2$. Then y_1 and y_1^2 are not fixed by any element in G , i.e.,

$$[K(x_1 + x_2, x_1 x_2, y_1) : K(x_1 + x_2, x_1 x_2)] = 4$$

and $K(x_1 + x_2, x_1 x_2, y_1) = K_m$. Now assume $G = \langle \tau_1, -\text{Id} \rangle$: since τ_1 does not fix ζ_m while $-\text{Id}$ does, we have

$$K(x_1, x_2) = K(x_1 + x_2, x_1 x_2, \zeta_m) .$$

Hence $K(x_1 + x_2, x_1 x_2, \zeta_m, y_1) = K(x_1, x_2, \zeta_m, y_1) = K_m$. □

Remark 2.9. The equality $K_2 = K(x_1 + x_2, x_1 x_2, \zeta_2, y_1)$ does not hold in general. Indeed it is equivalent to $K_2 = K(x_1 + x_2, x_1 x_2)$ and one can take $\mathcal{E} : y^2 = x^3 - 1$ (defined over \mathbb{Q}) and the points $\{P_1 = (\zeta_3, 0), P_2 = (\zeta_3^2, 0)\}$ (as a \mathbb{Z} -basis for $\mathcal{E}[2]$) to get $K_2 = \mathbb{Q}(\mu_3)$ and $\mathbb{Q}(x_1 + x_2, x_1 x_2) = \mathbb{Q}$. The equality would hold for any other basis, but the previous theorems allow total freedom in the choice of P_1 and P_2 .

3 The equality $K_m = K(x_1, \zeta_m, y_2)$

We start by proving the equality $K_m = K(x_1, \zeta_m, y_1, y_2)$ for every odd $m \geq 5$. The cases $m = 2, 3$ and 4 are treated in Remark 3.3, Section 5 and Section 6 respectively.

Theorem 3.1. *Let $m \geq 4$. If m is an odd number, then $K_m = K(x_1, \zeta_m, y_1, y_2)$. If m is an even number, then K_m is larger than $K(x_1, \zeta_m, y_1, y_2)$ if and only if $[K_m : K(x_1, \zeta_m, y_1, y_2)] = 2$ and its Galois group is generated by the element sending P_2 to $\frac{m}{2}P_1 + P_2$. In particular, if m is even then $K_{\frac{m}{2}} \subseteq K(x_1, \zeta_m, y_1, y_2)$.*

Proof. Let $\sigma \in \text{Gal}(K_m/K(x_1, \zeta_m, y_1, y_2))$ and write $\sigma(P_2) = \alpha P_1 + \beta P_2$ for some integers $0 \leq \alpha, \beta \leq m-1$. Since P_1 and ζ_m are σ -invariant we get

$$\zeta_m = \sigma(\zeta_m) = \sigma(e_m(P_1, P_2)) = \zeta_m^\beta ,$$

yielding $\beta = 1$ and $\sigma(P_2) = \alpha P_1 + P_2$. Since $K_m = K(x_1, \zeta_m, y_1, y_2, x_2)$ and x_2 is a root of $X^3 + AX + B - y_2^2$, the order of σ is at most 3. Assume now that $\sigma \neq \text{Id}$.

If the order of σ is 3: we have

$$P_2 = \sigma^3(P_2) = 3\alpha P_1 + P_2$$

hence $3\alpha \equiv 0 \pmod{m}$. Moreover, the three distinct points P_2 , $\sigma(P_2)$ and $\sigma^2(P_2)$ are on the line $y = y_2$. Thus their sum is zero, i.e.,

$$O = P_2 + \sigma(P_2) + \sigma^2(P_2) = 3\alpha P_1 + 3P_2 .$$

Since $3\alpha \equiv 0 \pmod{m}$, we deduce $3P_2 = O$, contradicting $m \geq 4$.

If the order of σ is 2: as above $P_2 = \sigma^2(P_2)$ yields $2\alpha \equiv 0 \pmod{m}$. If m is odd this implies $\alpha \equiv 0 \pmod{m}$, i.e., σ is the identity on $\mathcal{E}[m]$, a contradiction. If m is even the only possibility is $\alpha = \frac{m}{2}$.

The last statement for m even follows from the fact that σ acts trivially on $2P_1$ and $2P_2$. □

Corollary 3.2. *Let $p \geq 5$ be prime, then $[K_p : K(\zeta_p, y_1, y_2)]$ is odd.*

Proof. Assume there is a $\sigma \in \text{Gal}(K_p/K(\zeta_p, y_1, y_2))$ of order 2. For $i \in \{1, 2\}$, since $y_i \neq 0$ (because $p \neq 2$), one has $\sigma(P_i) \neq -P_i$ and $\sigma(P_i) + P_i$ is a nontrivial p -torsion point lying on the line $y = -y_i$. If $\sigma(P_i) + P_i$ is not a multiple of P_j ($i \neq j$); then the set $\{P_j, \sigma(P_i) + P_i\}$ is a basis of $\mathcal{E}[p]$. Let $\sigma(P_i) + P_i =: (\tilde{x}_i, -y_i)$; then by Theorem 3.1, we have $K(\zeta_p, \tilde{x}_i, y_1, y_2) = K_p$. But σ acts trivially on ζ_p, y_1 and y_2 by definition and on \tilde{x}_i as well (because $\sigma(\sigma(P_i) + P_i) = P_i + \sigma(P_i)$). Hence σ fixes K_p which contradicts $\sigma \neq \text{Id}$.

Therefore $\sigma(P_1) = -P_1 + \beta_1 P_2$ and $\sigma(P_2) = \beta_2 P_1 - P_2$ which, together with $\sigma^2 = \text{Id}$, yield $\beta_1 = \beta_2 = 0$. Hence both P_1 and P_2 are mapped to their opposite: a contradiction to $\sigma(y_i) = y_i$. \square

Remark 3.3. The equality $K_2 = K(x_1, \zeta_2, y_1, y_2)$ does not hold in general. A counterexample is again provided by the curve $\mathcal{E} : y^2 = x^3 - 1$ with $P_1 = (1, 0)$ (as in Remark 2.9 any other choice would yield the equality $K_2 = K(x_1)$).

Before going to the main theorem we show a little application for primes $p \equiv 2 \pmod{3}$.

Theorem 3.4. *Let $p \equiv 2 \pmod{3}$ be an odd prime, then $K_p = K(x_1, y_1, y_2)$ or $K_p = K(x_1, y_1, \zeta_p)$.*

Proof. The degree of x_2 over $K(y_2)$ is at most 3, hence $[K_p : K(x_1, y_1, y_2)] \leq 3$. By Theorem 3.1 we have the equality $K_p = K(x_1, \zeta_p, y_1, y_2)$ and the hypothesis ensures that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ is not divisible by 3, so the same holds for $[K_p : K(x_1, y_1, y_2)]$. Thus either $K_p = K(x_1, y_1, y_2)$ or $[K_p : K(x_1, y_1, y_2)] = 2$. If the second case occurs, then take the nontrivial element σ of $\text{Gal}(K_p/K(x_1, y_1, y_2))$. Since σ fixes x_1, y_1 and y_2 , it can be written as

$$\sigma = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \quad \text{with} \quad \sigma^2 = \begin{pmatrix} 1 & b(1+d) \\ 0 & d^2 \end{pmatrix}.$$

Since p is an odd prime, then $\sigma^2 = \text{Id}$ leads either to $d = 1$ (hence $b = 0$ and $\sigma = \text{Id}$, a contradiction) or to $d = -1$. Hence $\sigma(P_2) = bP_1 - P_2$ (with $b \neq 0$ otherwise σ would fix x_2 as well), i.e., bP_1 lies on the line $y = -y_2$. Thus $K(y_2) \subseteq K(x_1, y_1)$ and so $K_p = K(x_1, y_1, \zeta_p)$. \square

Corollary 3.5. *Let $p \equiv 2 \pmod{3}$ be an odd prime. Assume that \mathcal{E} has a K -rational torsion point P_1 of order p . Then either $K_p = K(\zeta_p)$ or $K_p = K(y_2)$.*

We are now ready to prove the equality appearing in the title of this section.

Theorem 3.6. *If $m \geq 4$ and $K_m = K(x_1, \zeta_m, y_1, y_2)$, then $K_m = K(x_1, \zeta_m, y_2)$ (in particular this holds for any odd $m \geq 5$, by Theorem 3.1).*

Proof. The hypotheses imply $K_m = K(x_1, \zeta_m, y_2)(y_1)$ so $[K_m : K(x_1, \zeta_m, y_2)] \leq 2$. Take $\sigma \in \text{Gal}(K_m/K(x_1, \zeta_m, y_2))$, then $\sigma(x_1) = x_1$ yields $\sigma(P_1) = \pm P_1$. If $\sigma(P_1) = P_1$, then $y_1 \in K(x_1, \zeta_m, y_2)$ and $K_m = K(x_1, \zeta_m, y_2)$. Assume that $\sigma(P_1) = -P_1$ and let

$$\sigma = \begin{pmatrix} -1 & a \\ 0 & b \end{pmatrix}.$$

Using the Weil pairing (recall $\zeta_m := e_m(P_1, P_2)$), we have $\zeta_m = \sigma(\zeta_m) = \zeta_m^{-b}$, which yields $b \equiv -1 \pmod{m}$, while

$$\sigma^2 = \begin{pmatrix} 1 & -2a \\ 0 & 1 \end{pmatrix} = \text{Id}$$

leads to $2a \equiv 0 \pmod{m}$.

Case $a \equiv 0 \pmod{m}$: we have $\sigma = -\text{Id}$. Then $\sigma(P_2) = -P_2$, i.e., $\sigma(x_2) = x_2 \in K(x_1, \zeta_m, y_2)$. By Theorem 2.5, this yields $K_m = K(x_1, \zeta_m, y_2)$ and contradicts $\sigma \neq \text{Id}$.

Case $a \equiv \frac{m}{2} \pmod{m}$: we have $\sigma(P_2) = \frac{m}{2}P_1 - P_2$, i.e., $\sigma(P_2) + P_2 - \frac{m}{2}P_1 = O$. Since P_2 and $\sigma(P_2)$ lie on the line $y = y_2$ and are distinct, then $-\frac{m}{2}P_1$ must be the third point of \mathcal{E} on that line. Since $-\frac{m}{2}P_1$ has order 2 this yields $y_2 = 0$, contradicting $m \geq 4$. \square

To provide generators for a more general m one can also use the following lemma.

Lemma 3.7.

1. Assume that $P \in E(K)$ is not a 2-torsion point and that $\phi : E \rightarrow E$ is a K -rational isogeny with $\phi(R) = P$. Then $K(x(R), y(R)) = K(x(R))$.
2. If R is a point in $\mathcal{E}(\overline{K})$ and $n \geq 1$, then we have $x(nR) \in K(x(R))$.

Proof. Part 1 is [12, Lemma 2.2] and part 2 is well known. \square

Proposition 3.8. Let m be divisible by $d \geq 3$ and let R be a point of order m . Then

$$K(x(R), y(R)) = K\left(x(R), y\left(\frac{m}{d}R\right)\right).$$

In particular, if $K = K(\mathcal{E}[d])$ and R is a point of order m , then $K(x(R), y(R)) = K(x(R))$.

Proof. Apply the previous lemma to the field $K(P)$, with $P = \frac{m}{d}R$ and $\phi = [\frac{m}{d}]$. \square

Corollary 3.9. Let m be divisible by an odd number $d \geq 5$. Then

$$K_m = K\left(x(P_1), x(P_2), \zeta_d, y\left(\frac{m}{d}P_2\right)\right).$$

Proof. By Proposition 3.8, $K_m = K_d(x(P_1), x(P_2))$. Obviously $\{\frac{m}{d}P_1, \frac{m}{d}P_2\}$ is a \mathbb{Z} -basis for $\mathcal{E}[d]$, hence Theorem 3.1 and Theorem 3.6 (applied with $m = d$) yield

$$K_d = K\left(x\left(\frac{m}{d}P_1\right), \zeta_d, y\left(\frac{m}{d}P_2\right)\right).$$

By Lemma 3.7, we have $x(\frac{m}{d}P_1) \in K(x(P_1))$ and the corollary follows. \square

The previous result leaves out only integers m of the type $2^s 3^t$. For the case $t = 1$ we mention the following

Proposition 3.10. Assume $\text{char}(K) \neq 2, 3$, then the coordinates of the points of order dividing $3 \cdot 2^n$ can be explicitly computed by radicals out of the coefficients of the Weierstrass equation.

Proof. By the Weierstrass equation, we can compute the y -coordinates out of the x -coordinate. Then by the addition formula, it suffices to compute the x -coordinate of two \mathbb{Z} -independent points of order 3 (done in Section 5), and the x -coordinate of two \mathbb{Z} -independent points of order 2^n (done in Section 6 for $n = 1, 2$). The coordinate $x(P)$ of a point P of order 2^n (with $n \geq 3$) can be computed from $x(2P)$. Indeed, we have $y(P) \neq 0$ (because the order of P is not 2) and so, by the duplication formula,

$$x(2P) = \frac{x(P)^4 - 2Ax(P)^2 - 8Bx(P) + A^2}{4x(P)^3 + 4Ax(P) + 4B}$$

(a polynomial equation of degree 4 with coefficients coming from the Weierstrass equation). \square

Proposition 3.11. *If m is divisible by 3 (resp. 4), then*

$$K_m = K_{m,x} \cdot K(y(Q_1), y(Q_2))$$

where $\{Q_1, Q_2\}$ is a \mathbb{Z} -basis for $\mathcal{E}[3]$ (resp. $\mathcal{E}[4]$).

Proof. Just apply Proposition 3.8 with $d = 3$ (resp. $d = 4$). □

4 Galois representations and exceptional primes

We begin with some remarks on the Galois group $\text{Gal}(K_p/K)$ for a prime $p \geq 5$, which led us to believe that the generating set $\{x_1, \zeta_p, y_2\}$ is often minimal.

Lemma 4.1. *For any prime $p \geq 5$ one has $[K_p : K(x_1, \zeta_p)] \leq 2p$. Moreover the Galois group $\text{Gal}(K_p/K(x_1, \zeta_p))$ is cyclic, generated by a power of $\eta = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$.*

Proof. By Theorem 3.6, we have $K_p = K(x_1, \zeta_p, y_2)$. Let $\sigma \in \text{Gal}(K_p/K(x_1, \zeta_p))$, then $\sigma(P_1) = \pm P_1$ and $\det(\sigma) = 1$ yield $\sigma = \begin{pmatrix} \pm 1 & \alpha \\ 0 & \pm 1 \end{pmatrix}$ (for some $0 \leq \alpha \leq p-1$). The powers of η are

$$\eta^n = \begin{cases} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} & \text{if } n \text{ is even} \\ \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} & \text{if } n \text{ is odd} \end{cases}$$

and its order is obviously $2p$; clearly any such σ is a power of η . □

Remark 4.2. The group generated by η in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is not normal; hence, in general, the extension $K(x_1, \zeta_p)/K$ is not Galois.

Since the p -th division polynomial has degree $\frac{p^2-1}{2}$ and, obviously, $[K(x_1, \zeta_p) : K(x_1)] \leq p-1$ one immediately finds

$$[K(x_1, \zeta_p, y_2) : K] \leq \frac{p^2-1}{2} \cdot (p-1) \cdot 2p = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})|$$

and can provide conditions for the equality to hold.

Theorem 4.3. *Let $p \geq 5$ be a prime, then $\text{Gal}(K_p/K) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ if and only if the following hold:*

1. $\zeta_p \notin K$;
2. the p -th division polynomial φ_p is irreducible in $K(\zeta_p)[x]$;
3. $y_1 \notin K(\zeta_p, x_1)$ and the generator of $\text{Gal}(K(\zeta_p, x_1, y_1)/K(\zeta_p, x_1))$ is not $-\text{Id}$.

Proof. Let σ be a generator of $\text{Gal}(K(\zeta_p, x_1, y_1)/K(\zeta_p, x_1))$. Then $\sigma(P_1) = -P_1$ (because of hypothesis 3) and $\det(\sigma) = 1$. Hence it is of type $\sigma = \begin{pmatrix} -1 & \alpha \\ 0 & -1 \end{pmatrix}$ with $\alpha \neq 0$ (again by hypothesis 3). Therefore σ has order $2p$ in $\text{Gal}(K_p/K(\zeta_p, x_1))$ and the hypotheses lead to the equality $[K_p : K] = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})|$. Vice versa it is obvious that if any of the conditions does not hold we get $[K_p : K] < |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})|$. □

Remark 4.4. As mentioned in the Introduction, if K is a number field and \mathcal{E} has no complex multiplication, then one expects the equality to hold for almost all primes p (for a recent bound on exceptional primes for which $\rho_{\mathcal{E},p}$ is not surjective see [9]). Hence for a general number field K (which, of course, can contain ζ_p or some coordinates of generators of $\mathcal{E}[p]$ only for finitely many p) one expects $\{x_1, \zeta_p, y_2\}$ to be a minimal set of generators for K_p over K (among those contained in $\{x_1, x_2, y_1, y_2, \zeta_p\}$). We have encountered an exceptional case in Theorem 3.4, where for $p \equiv 2 \pmod{3}$ ($p \neq 2$) one could have $K_p = K(x_1, y_1, \zeta_p)$. If this is the case, the maximum degree for $[K_p : K]$ is $\frac{p^2-1}{2} \cdot 2 \cdot (p-1)$. Therefore for infinitely many primes $p \equiv 2 \pmod{3}$ we have $K_p = K(x_1, y_1, y_2) = K(x_1, \zeta_p, y_2) \neq K(x_1, y_1, \zeta_p)$ (which emphasizes the need for coordinates of P_2 in our generating set).

Definition 4.5. For an elliptic curve \mathcal{E} defined over a number field K and a prime p we say that p is *exceptional* for \mathcal{E} if $\rho_{\mathcal{E},p}$ is not surjective, i.e., if $[K_p : K] < |\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$. In particular, if \mathcal{E} has complex multiplication, then all primes are exceptional for \mathcal{E} , because K_p/K is an abelian extension (see, e.g., [18, Chapter II, §5]).

In the rest of this Section 4 we will investigate the case of exceptional primes, assuming that K is a number field. For exceptional primes the Galois group $\mathrm{Gal}(K_p/K)$ is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Hence it falls in one of the following cases (see [14, Section 2] for a complete proof or [9, Lemma 4] for a similar statement).

Lemma 4.6. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ then one of the following holds:*

1. *G is contained in a Borel subgroup;*
2. *G is a Cartan subgroup;*
3. *G is contained in the normalizer of a Cartan subgroup, but it is not a Cartan subgroup;*
4. *the image of G under the projection $\pi : \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \rightarrow \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is contained in a subgroup which is isomorphic to one of the alternating groups A_4 and A_5 or to the symmetric group S_4 .*

In particular if one of cases **1** or **2** holds, then G acts reducibly on $\mathcal{E}[p]$. Regarding case **4** we have the next statement.

Lemma 4.7. *If $p \geq 53$ is unramified in K/\mathbb{Q} and exceptional for \mathcal{E} , then $\mathrm{Gal}(K_p/K)$ does not satisfy **4** of Lemma 4.6.*

Proof. See [9, Lemma 8], depending on [15, Lemma 18]. □

We shall provide some information on the generating sets for K_p when p is exceptional for \mathcal{E} and $\mathrm{Gal}(K_p/K)$ falls in cases **1**, **2** or **3** of Lemma 4.6. We start with the already mentioned exceptional case appearing in Theorem 3.4 and recall that we are always assuming $p \geq 5$.

Proposition 4.8. *If $K_p = K(x_1, y_1, \zeta_p)$, then $[K_p : K] < (p^2 - 1)(p - 1)$ unless $p = 5$ and $\pi(\mathrm{Gal}(K_p/K)) \simeq S_4$.*

Proof. We have already noticed that $[K_p : K] \leq (p^2 - 1)(p - 1)$, so the prime p is exceptional. But the order of a Borel subgroup is $p(p - 1)^2$ and the order of a Cartan subgroup is at most $(p - 1)^2$ (and it has index 2 in its normalizer), so the statement holds (even with the stronger bound $p(p - 1)^2$) when $\mathrm{Gal}(K_p/K)$ falls in cases **1**, **2** or **3** of Lemma 4.6. Assume we are in case **4** and note that if $|\mathrm{Gal}(K_p/K)| = (p^2 - 1)(p - 1)$, then $|\pi(\mathrm{Gal}(K_p/K))| \geq p^2 - 1$. Thus case **4** cannot happen for $p \geq 11$. Moreover, if $p = 7$, then $p^2 - 1 > |S_4|$ and $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ does not contain $|A_5|$ (see [14, Section 2.5]). We are left with $p = 5$, $[K_5 : K] = 96$ and $|\pi(\mathrm{Gal}(K_p/K))| \geq 24 = |S_4|$, which completes the proof. □

4.1 Exceptional primes I: Borel subgroup

Assume that $p \geq 5$ is exceptional for \mathcal{E} and $\text{Gal}(K_p/K)$ is contained in a Borel subgroup. We can write elements of $\text{Gal}(K_p/K)$ as upper triangular matrices $\sigma = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ with $ac \neq 0$ (this is not restrictive, since the results of the previous sections were completely independent of the chosen basis $\{P_1, P_2\}$).

Theorem 4.9. *Let $p \geq 5$ and assume that $\text{Gal}(K_p/K)$ is contained in a Borel subgroup.*

1. *If $p \not\equiv 1 \pmod{3}$, then $K_p = K(\zeta_p, y_2)$;*
2. *if $p \equiv 1 \pmod{3}$, then $[K_p : K(\zeta_p, y_2)]$ is 1 or 3.*

Proof. We know $K_p = K(x_1, \zeta_p, y_2)$. Take an element $\sigma \in \text{Gal}(K_p/K(\zeta_p, y_2))$ so that $\sigma = \begin{pmatrix} a^{-1} & b \\ 0 & a \end{pmatrix}$. Let P_2, R_2 and S_2 be the three points of the curve \mathcal{E} on the line $y = y_2$, so that $P_2 + R_2 + S_2 = O$. We have that $\sigma(P_2) = bP_1 + aP_2$ must be P_2 or R_2 or S_2 (the cases R_2 and S_2 are obviously symmetric).

Case 1: $\sigma(P_2) = P_2$. Then $b = 0$, $a = 1$ and $\sigma = \text{Id}$.

Case 2: $\sigma(P_2) = R_2$. Then $\sigma^2(P_2) = a^{-1}bP_1 + abP_1 + a^2P_2$.

- If $\sigma^2(P_2) = P_2$, then $a^2 = 1$ and $a + a^{-1} \neq 0$ yields $b = 0$. Hence $\sigma(P_1) = \pm P_1$ and σ fixes x_1 . Since $K_p = K(x_1, \zeta_p, y_2)$, this implies $\sigma = \text{Id}$.
- If $\sigma^2(P_2) = R_2$, then one gets $a^2 = a$ (i.e., $a = 1$) and $2b = b$ (i.e., $b = 0$), leading to $\sigma = \text{Id}$.
- If $\sigma^2(P_2) = S_2$, then $P_2 + R_2 + S_2 = O$ yields

$$P_2 + bP_1 + aP_2 + a^{-1}bP_1 + abP_1 + a^2P_2 = ba^{-1}(a + 1 + a^2)P_1 + (1 + a + a^2)P_2 = O$$

Thus $1 + a + a^2 = 0$ and this is possible if and only if $p \equiv 1 \pmod{3}$.

Therefore, if $p \not\equiv 1 \pmod{3}$, we have $\sigma = \text{Id}$ and $K_p = K(\zeta_p, y_2)$. If $p \equiv 1 \pmod{3}$ and $1 + a + a^2 = 0$, then the above σ has order 3 and the proof is complete. \square

4.2 Exceptional primes II: Cartan subgroup

Assume that $p \geq 5$ is exceptional for \mathcal{E} and $\text{Gal}(K_p/K)$ is contained in a Cartan subgroup (resp. in a normalizer of a Cartan subgroup). Then we can write elements of $\text{Gal}(K_p/K)$ as matrices $\sigma = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$ (resp. $\sigma = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$ or $\sigma = \begin{pmatrix} 0 & a \\ c & 0 \end{pmatrix}$) with $ac \neq 0$.

Theorem 4.10. *In the above setting we have $K_p = K(x_1, \zeta_p)$ or $K(x_1, y_1, \zeta_p)$. Moreover*

1. *if $p \not\equiv 1 \pmod{3}$, then $K_p = K(\zeta_p, y_2)$;*
2. *if $p \equiv 1 \pmod{3}$, then $[K_p : K(\zeta_p, y_2)]$ is 1 or 3.*

Proof. Note that the only elements of the normalizer of a Cartan subgroup (hence, in particular, of a Cartan subgroup) which fix x_1 and ζ_p are $\pm \text{Id}$: the first statement follows immediately. Now consider $\sigma \in \text{Gal}(K_p/K(\zeta_p, y_2))$ and let R_2 and S_2 be the points defined in Theorem 4.9.

If $\sigma = \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$, then $\sigma^2(P_2) = \sigma(aP_1) = -P_2$. Since σ fixes y_2 , this implies $y_2 = 0$

which contradicts $p \neq 2$. Therefore we can restrict to Cartan subgroups and consider only $\sigma = \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}$.

Case 1: $\sigma(P_2) = P_2$. Then $a = 1$ and $\sigma = \text{Id}$.

Case 2: $\sigma(P_2) = R_2$. Then $\sigma^2(P_2) = a^2 P_2$.

- If $\sigma^2(P_2) = P_2$, then $a^2 = 1$ and $\sigma(P_1) = \pm P_1$. As in Theorem 4.9, this implies $\sigma = \text{Id}$.
- If $\sigma^2(P_2) = R_2$, then $a^2 = a$ yields $a = 1$ and $\sigma = \text{Id}$.
- If $\sigma^2(P_2) = S_2$, then $P_2 + R_2 + S_2 = O$ yields

$$P_2 + aP_2 + a^2P_2 = (1 + a + a^2)P_2 = O.$$

Thus $1 + a + a^2 = 0$ and this is possible if and only if $p \equiv 1 \pmod{3}$.

Therefore, if $p \not\equiv 1 \pmod{3}$, we have $\sigma = \text{Id}$ and $K_p = K(\zeta_p, y_2)$. If $p \equiv 1 \pmod{3}$ and $1 + a + a^2 = 0$, then σ has order 3. \square

Remark 4.11. The information carried by ζ_p seems more relevant than that by the coordinate x_1 in the exceptional case. Indeed if one considers a $\sigma \in \text{Gal}(K_p/K(x_1, y_2))$, there is always room for elements like $\sigma = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ of order 2. A proof similar to the previous ones leads to (both in the Borel and the Cartan case)

1. $p \not\equiv 1 \pmod{3} \implies [K_p : K(x_1, y_2)]$ divides 4;
2. $p \equiv 1 \pmod{3} \implies [K_p : K(x_1, y_2)]$ divides 12.

4.3 Remarks on modular curves

We give just an application of the results of the previous sections to the classical modular curves $X(p)$ and $X_1(p)$, associated to the action of the congruence subgroups

$$\Gamma(p) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p} \right\}$$

and

$$\Gamma_1(p) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{p} \right\}$$

on the complex upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \text{Im } z > 0\}$ via Möbius transformations (for detailed definitions and properties see, e.g. [8] or [16]). We recall that $X(p)$ and $X_1(p)$ parametrize families of elliptic curves with some extra *level p structure* via their moduli interpretation. Namely

- non cuspidal points in $X(p)$ correspond to triples (\mathcal{E}, P_1, P_2) where \mathcal{E} is an elliptic curve (defined over \mathbb{C}) and P_1, P_2 are points of order p generating the whole group $\mathcal{E}[p]$;
- non cuspidal points in $X_1(p)$ correspond to couples (\mathcal{E}, Q) where \mathcal{E} is an elliptic curve (defined over \mathbb{C}) and Q is a point of order p

(all these correspondences have to be considered modulo the natural isomorphisms).

Let K be a number field. The points of $X(p)$ or $X_1(p)$ which are rational over K will be denoted by $X(p)(K)$ or $X_1(p)(K)$. Obviously a point is K -rational if and only if it is $\text{Gal}(\overline{\mathbb{Q}}/K)$ -invariant (in particular, with the representation provided above one needs an elliptic curve \mathcal{E} defined over K).

Definition 4.12. A point $(\mathcal{E}, P_1, P_2) \in X(p)$ (resp. $(\mathcal{E}, P_1) \in X_1(p)$) is said to be *exceptional* if p is exceptional for \mathcal{E} . In particular, if \mathcal{E} is defined over K , we call such a point *Borel exceptional* (resp. *Cartan exceptional*) if $\text{Gal}(K(\mathcal{E}[p])/K)$ is contained in a Borel subgroup (resp. in the normalizer of a Cartan subgroup).

The following is an easy consequence of Theorem 3.6.

Corollary 4.13. Assume $p \geq 5$; let \mathcal{E} be an elliptic curve defined over a number field K and let $P \in \mathcal{E}[p]$ be of order p . For any field L containing $K(x(P), \zeta_p)$ or containing $K(y(P), \zeta_p)$ and for any point $Q \in \mathcal{E}[p]$ independent from P , we have

$$(\mathcal{E}, Q) \in X_1(p)(L) \iff (\mathcal{E}, P, Q) \in X(p)(L) .$$

Proof. The arrow \Leftarrow is obvious. Now assume $(\mathcal{E}, Q) \in X_1(p)(L)$, then

$$L \supseteq K(x(P), \zeta_p, y(Q)) = K_p \quad \text{or} \quad L \supseteq K(y(P), \zeta_p, x(Q)) = K_p$$

(both final equalities hold because of Theorem 3.6). Hence $(\mathcal{E}, P, Q) \in X(p)(L)$. \square

It would be interesting to describe the families of elliptic curves for which the previous corollary becomes trivial, i.e., curves for which $K(x(P), \zeta_p)$ or $K(y(P), \zeta_p)$ contain $K(x(P), y(P))$. Some examples are provided by the exceptional primes $\equiv 1 \pmod{3}$ for which $K(\zeta_p, y(P)) = K_p$.

On exceptional points we have the following

Corollary 4.14. Assume $p \geq 53$ is unramified in K/\mathbb{Q} and $p \not\equiv 1 \pmod{3}$, then, for any field $L \supseteq K(\zeta_p)$, the L -rational exceptional points of $X(p)$ and $X_1(p)$ are associated to the same elliptic curves. The same statement holds for $p \equiv 1 \pmod{3}$ as well if we restrict to Cartan exceptional points.

Proof. We only need to check that if $(\mathcal{E}, Q) \in X_1(p)(L)$ is exceptional, then $(\mathcal{E}, Q, R) \in X(p)(L)$, for any R completing Q to a \mathbb{Z} -basis of $\mathcal{E}[p]$. For $p \not\equiv 1 \pmod{3}$, this immediately follows from

$$L \supseteq K(\zeta_p, y(Q)) = K_p,$$

by Theorems 4.9 and 4.10. If $p \equiv 1 \pmod{3}$ (and (\mathcal{E}, Q) is Cartan exceptional), then Theorem 4.10 shows that

$$L \supseteq K(\zeta_p, x(P), y(Q)) = K_p . \quad \square$$

5 Fields $K(\mathcal{E}[3])$

In this section we generalize the classification of the number fields $\mathbb{Q}(\mathcal{E}[3])$, appearing in [4], to the case when the characteristic of the base field K is different from 2 and 3. Under the last assumption on K we have that \mathcal{E} can be written in Weierstrass form $y^2 = x^3 + Ax + B$. We recall that the four x -coordinates of the 3-torsion points of \mathcal{E} are the roots of the polynomial $\varphi_3 := x^4 + 2Ax^2 + 4Bx - A^2/3$. Solving φ_3 with radicals, we get explicit expressions for the x -coordinates and we recall that for $m = 3$ being \mathbb{Z} -independent is equivalent to having

different x -coordinates. Let $\Delta := -432B^2 - 64A^3$ be the discriminant of the elliptic curve. If $B \neq 0$, the roots of φ_3 are

$$\begin{aligned} x_1 &= -\frac{1}{2}\sqrt{\frac{\sqrt[3]{\Delta}-8A}{3}-\frac{8B\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta}-4A}}}+\frac{\sqrt{-\sqrt[3]{\Delta}-4A}}{2\sqrt{3}}, \\ x_2 &= \frac{1}{2}\sqrt{\frac{\sqrt[3]{\Delta}-8A}{3}-\frac{8B\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta}-4A}}}+\frac{\sqrt{-\sqrt[3]{\Delta}-4A}}{2\sqrt{3}}, \\ x_3 &= -\frac{1}{2}\sqrt{\frac{\sqrt[3]{\Delta}-8A}{3}+\frac{8B\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta}-4A}}}-\frac{\sqrt{-\sqrt[3]{\Delta}-4A}}{2\sqrt{3}}, \\ x_4 &= \frac{1}{2}\sqrt{\frac{\sqrt[3]{\Delta}-8A}{3}+\frac{8B\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta}-4A}}}-\frac{\sqrt{-\sqrt[3]{\Delta}-4A}}{2\sqrt{3}}. \end{aligned}$$

(where we have chosen one square root of γ and one cubic root for Δ ; since $\zeta_3 \in K_3$ the degree $[K_3 : K]$ will not depend on this choice).

To ease notation, we define

$$\gamma := \frac{-\sqrt[3]{\Delta}-4A}{3}, \quad \delta := \frac{(-\gamma-4A)\sqrt{\gamma}-8B}{\sqrt{\gamma}} \quad \text{and} \quad \delta' := \frac{(-\gamma-4A)\sqrt{\gamma}+8B}{\sqrt{\gamma}}.$$

Thus, when $B \neq 0$, the roots of φ_3 are

$$x_1 = \frac{1}{2}(-\sqrt{\delta} + \sqrt{\gamma}), \quad x_2 = \frac{1}{2}(\sqrt{\delta} + \sqrt{\gamma}), \quad x_3 = \frac{1}{2}(-\sqrt{\delta'} - \sqrt{\gamma}) \quad \text{and} \quad x_4 = \frac{1}{2}(\sqrt{\delta'} - \sqrt{\gamma}).$$

The corresponding points $P_i := (x_i, \sqrt{x_i^3 + Ax_i + B})$ have order 3 and are pairwise \mathbb{Z} -independent (this would hold with any choice for the sign of the square root providing the y -coordinate). For completeness, we show the expressions of y_1, y_2, y_3 and y_4 in terms of A, B, γ, δ and δ' :

$$\begin{aligned} y_1 &= \sqrt{\frac{(-\gamma\sqrt{\gamma}+4B)\sqrt{\delta}+\gamma\delta}{4\sqrt{\gamma}}}, \quad y_2 := \sqrt{\frac{(\gamma\sqrt{\gamma}-4B)\sqrt{\delta}+\gamma\delta}{4\sqrt{\gamma}}}, \\ y_3 &= \sqrt{\frac{(-\gamma\sqrt{\gamma}-4B)\sqrt{\delta'}-\gamma\delta'}{4\sqrt{\gamma}}}, \quad y_4 = \sqrt{\frac{(\gamma\sqrt{\gamma}+4B)\sqrt{\delta'}-\gamma\delta'}{4\sqrt{\gamma}}}. \end{aligned}$$

If $B = 0$, then $\gamma = 0$ too and the formulas provided above do not hold anymore. The x -coordinates are now the roots of $\varphi_3 = x^4 + 2Ax^2 - A^2/3$. Let

$$\beta := -\left(\frac{2\sqrt{3}}{3} + 1\right)A \quad \text{and} \quad \eta := \left(\frac{2\sqrt{3}}{3} - 1\right)A,$$

then the roots of φ_3 are $x_1 = \sqrt{\beta}, x_2 = -\sqrt{\beta}, x_3 = \sqrt{\eta}$ and $x_4 = -\sqrt{\eta}$. Furthermore

$$y_1 = \sqrt{\frac{-2A\sqrt{\beta}}{\sqrt{3}}} = \sqrt{\frac{-2A}{3}}\sqrt{-2A\sqrt{3}-3A}.$$

Using the results of the previous sections and the explicit formulas, we can now give the following description of K_3 in terms of generators.

Proposition 5.1. *In any case $K_3 = K(x_1, y_1, y_2)$. Moreover*

1. *if $B \neq 0$, then $K_3 = K(\sqrt{\gamma}, \zeta_3, y_1)$;*
2. *if $B = 0$, then $K_3 = K(\zeta_3, y_1)$.*

Proof. If $B \neq 0$, then

$$y_1^2 + y_2^2 = -4B - \frac{\gamma^2}{2\sqrt{\gamma}} - 2A\sqrt{\gamma}.$$

Therefore $x_1 + x_2 = \sqrt{\gamma} \in K(y_1^2, y_2^2)$ and $x_2 \in K(x_1, y_1^2, y_2^2)$, which immediately yields $K_3 = K(x_1, y_1, y_2)$. Moreover, by Theorem 2.8, $K_3 = K(x_1 + x_2, x_1x_2, \zeta_3, y_1)$. So, since

$$x_1x_2 = \frac{\gamma}{2} + A + \frac{2B}{\sqrt{\gamma}} \in K(x_1 + x_2) = K(\sqrt{\gamma}),$$

one has $K_3 = K(\sqrt{\gamma}, \zeta_3, y_1)$.

If $B = 0$, then $x_1 = \sqrt{\beta} = -x_2$ so $K_3 = K(x_1, y_1, y_2)$ is obvious. The final statement follows from $x_1 + x_2 = 0$, $K(x_1x_2) = K(\sqrt{\beta}) \subseteq K(y_1)$ and Theorem 2.8. \square

We shall use the statements of Proposition 5.1 to describe the fields K_3 in terms of the degree $[K_3 : K]$ and the Galois groups $\text{Gal}(K_3/K)$.

5.1 The degree $[K_3 : K]$

Because of the embedding

$$\text{Gal}(K_n/K) \hookrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

one has that $[K_3 : K]$ is a divisor of $|\text{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 48$ (in particular, if $B = 0$, then $K_3 = K(\zeta_3, y_1)$ and y_1 has degree at most 8 over K so $d := [K_3 : K]$ divides 16). Therefore $d \in \Omega := \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$. In [4], we proved that the minimal set for $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}]$ is $\tilde{\Omega} := \{2, 4, 6, 8, 12, 16, 48\}$ and showed also explicit examples for any degree $d \in \tilde{\Omega}$. When K is a number field we can get also examples of degree 1, 3 and 24: it suffices to take the curves in [4] with degree $d \in \{2, 6, 48\}$ and choose $K = \mathbb{Q}(\zeta_3)$ as base field. In general, once we have a curve \mathcal{E} defined over \mathbb{Q} with $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 48$, we produce examples of any degree $d \in \Omega$ by simply considering the same curve over subfields K of $\mathbb{Q}(\mathcal{E}[3])$ (obviously for those K one has $K_3 = \mathbb{Q}(\mathcal{E}[3])$).

Theorem 5.2. *With notations as above let $d := [K_3 : K]$. Consider the following conditions for $B \neq 0$*

- | | | |
|---|--|--|
| A1. $\sqrt[3]{\Delta} \notin K$; | B1. $\sqrt{\delta} \notin K(\sqrt{\gamma})$; | C. $\zeta_3 \notin K(\sqrt{\gamma}, y_1)$; |
| A2. $\sqrt{\gamma} \notin K(\sqrt[3]{\Delta})$; | B2. $y_1 \notin K(\sqrt{\delta})$; | |

and the corresponding ones for $B = 0$

- | | |
|--|-------------------------------------|
| D1. $\sqrt{3} \notin K$; | E. $\zeta_3 \notin K(y_1)$; |
| D2. $\sqrt{\beta} \notin K(\sqrt{3})$; | |
| D3. $y_1 \notin K(\sqrt{\beta})$. | |

Then the degrees are the following

B	d	holding conditions	B	d	holding conditions
$\neq 0$	48	A1, A2, B1, B2, C	$\neq 0$	4	A2, B1
$\neq 0$	24	A1, B1, B2, C	$\neq 0$	4	A2, B2
$\neq 0$	24	A1, A2, B1, B2	$\neq 0$	4	B1, B2
$\neq 0$	16	A2, B1, B2, C	$\neq 0$	3	A1
$\neq 0$	12	A1, A2, B1	$\neq 0$	2	<i>1 among A2, B1, B2</i>
$\neq 0$	12	A1, A2, B2	0	16	D1, D2, D3, E
$\neq 0$	12	A1, B1, B2	0	8	D2, D3, E
$\neq 0$	8	B1, B2, C	0	4	D1, D3
$\neq 0$	8	A2, B1, B2	0	4	D2, D3
$\neq 0$	6	A1 and 1 among A2, B1, B2	0	2	D1
			0	2	D3

Proof. Everything follows from Proposition 5.1 and the explicit description of the generators of K_3 ; just note that all conditions (except **A1** which provides an extension of degree 3) yield extensions of degree 2. We remark that not all possible combinations appear in the table because there are certain relations between the conditions. Indeed, for $B = 0$, condition **D2** implies condition **D3** (since $y_1 = \sqrt{\frac{2A}{\sqrt{3}}}\sqrt[4]{\beta}$), while, if **D2** does not hold, then $x_1 \in K(\sqrt{3})$ and $x_3 = \sqrt{\left(\frac{2\sqrt{3}}{3} - 1\right)A} \in K(\sqrt{3})$ as well. Since $x_1x_3 = \frac{A\sqrt{-3}}{3}$, this implies that **E** does not hold. In the same way one sees that if **B1** does not hold then δ and δ' are both squares in $K(\sqrt{\gamma})$. Therefore $x_i \in K(\sqrt{\gamma})$ for $1 \leq i \leq 4$ and, by (the proof of) Theorem 2.5, $\zeta_3 \in K(\sqrt{\gamma})$ as well, i.e., **C** does not hold. Moreover if **B2** does not hold, then y_1^2 , which is of the form $u + v\sqrt{\delta}$ for some $u, v \in K(\sqrt{\gamma})$, is a square in $K(\sqrt{\delta})$, hence $y_2^2 = u - v\sqrt{\delta}$ is a square as well. In this case we have $\sqrt{\gamma}, \sqrt{\delta}, y_1, y_2 \in K(\sqrt{\delta})$, i.e., $K_3 = K(x_1, y_1, y_2) = K(\sqrt{\delta})$ (in particular **C** does not hold). \square

5.2 Galois groups.

We now list all possible Galois groups $\text{Gal}(K_3/K)$ via a case by case analysis (one can easily connect a Galois group to the conditions in Theorem 5.2, so we do not write down a summarizing statement here).

5.2.1 $B = 0$

The degree $[K_3 : K]$ divides 16. Hence $\text{Gal}(K_3/K)$ is a subgroup of the 2-Sylow subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ which is isomorphic to SD_8 (the semidihedral group of order 16). If $d = 16$, then $\text{Gal}(K_3/K) \simeq SD_8$ and, by [4, Theorem 3.1], it is generated by the elements

$$\varphi_{6,1} \left\{ \begin{array}{l} y_1 \mapsto y_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \quad \text{and} \quad \varphi_{2,1} \left\{ \begin{array}{l} y_1 \mapsto y_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right.$$

(here and in what follows the notations for the $\varphi_{i,j}$ are taken from [4, Appendix A]).

Obviously if $d = 2$, then $\text{Gal}(K_3/K) \simeq \mathbb{Z}/2\mathbb{Z}$ and $d = 1$ yields a trivial group. Hence we are left with $d = 4$ and 8.

If $d = 8$: then $\sqrt{3} \in K$ but $\sqrt{-3} \notin K$ which yields $i \notin K$. Letting φ be any element of the Galois group, one has $\varphi(y_1^2) = \pm y_1^2$, i.e., $\varphi(y_1) = \pm y_1, \pm iy_1$. Then

$$\text{Gal}(K_3/K) = \langle \varphi_{6,1}^2, \varphi_{2,1} : \varphi_{6,1}^8 = \varphi_{2,1}^2 = \text{Id}, \varphi_{2,1}\varphi_{6,1}^2\varphi_{2,1} = \varphi_{6,1}^6 \rangle \simeq D_4$$

(the dihedral group of order 8).

If $d = 4$: then there are two cases

- a. $\sqrt{3} \notin K$, $\sqrt{\beta}, \zeta_3 \in K(\sqrt{3})$ and $y_1 \notin K(\sqrt{3})$, or
- b. $\sqrt{3} \in K$, $[K(y_1) : K] = 4$ and $\zeta_3 \in K(y_1)$.

In case **a** there are elements sending $\sqrt{3}$ to $-\sqrt{3}$, hence x_1 to x_3 and y_1^2 to $\pm y_3^2$. There are no such elements of order 2, so $\text{Gal}(K_3/K) \simeq \mathbb{Z}/4\mathbb{Z}$ and it is generated by $\varphi_{6,1}\varphi_{2,1}$ or $\varphi_{6,1}^3\varphi_{2,1}$ (note that both fix ζ_3 , hence one can also deduce that this case happens if ζ_3 belongs to K and i does not).

In case **b** (as in $d = 8$) one has $\varphi(y_1^2) = \pm y_1^2$. If $\zeta_3 \in K$, then $i \in K$ as well and the Galois group is $\langle \varphi_{6,1}^2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. If $\zeta_3 \notin K$, then the Galois group must contain elements moving i and, among them, the ones sending y_1^2 to $\pm y_1^2$. All such elements have order 2. Therefore $\text{Gal}(K_3/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the generators are $\{\varphi_{6,1}^4, \varphi_{2,1}\}$ or $\{\varphi_{6,1}^4, \varphi_{2,1}\varphi_{6,1}^6\}$.

5.2.2 $B \neq 0$

The degree is a divisor of 48. Looking at the subgroups of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ one sees that certain orders do not leave any choice: indeed $d = 1, 2, 3, 12, 16, 24$ and 48 give $\text{Gal}(K_3/K) \simeq \text{Id}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, D_6 , SD_8 , $\text{SL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ respectively. The remaining orders are $d = 4, 6$ and 8 .

If $d = 8$: then there are two cases

- a. $K = K(\sqrt{\gamma})$, $[K(y_1) : K] = 4$ and $K_3 = K(y_1, \zeta_3)$, or
- b. $K = K(\sqrt[3]{\Delta})$ and $K_3 = K(\sqrt{\gamma}, y_1)$.

In case **a**, since all elements of the Galois group fix $\sqrt{\gamma}$, one has $\varphi(\sqrt{\delta}) = \pm\sqrt{\delta}$, which yields $\varphi(y_1) \in \{\pm y_1, \pm y_2\}$. Therefore φ has order 1, 2 or 4 and, since $(\mathbb{Z}/2\mathbb{Z})^3$ is not a subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$, we have some elements of order 4 (the ones with $\varphi(y_1) = \pm y_2$). Moreover there is $\sigma \in \text{Gal}(K_3/K(y_1))$ with $\sigma(\zeta_3) = \zeta_3^2$. Note that in this case $x_1 \in K(y_1)$ so $y_2 \notin K(y_1)$ (otherwise $K_3 = K(y_1)$ by Proposition 5.1, a contradiction to $[K_3 : K] = 8$), hence $\sigma(y_2) = -y_2$. Now it is easy to check that $\text{Gal}(K_3/K) = \langle \varphi, \sigma : \varphi^4 = \sigma^2 = \text{Id}, \sigma\varphi\sigma = \varphi^3 \rangle \simeq D_4$, with

$$\varphi \begin{cases} y_1 \mapsto y_2 \\ \zeta_3 \mapsto \zeta_3 \end{cases} \quad \text{and} \quad \sigma \begin{cases} y_1 \mapsto y_1 \\ \zeta_3 \mapsto \zeta_3^2 \end{cases}.$$

In case **b**, since $\sqrt{\gamma}$ is no longer fixed, $\varphi(\delta) \in \{\delta, \delta'\}$ and therefore the image of y_1 can be any of the other y_i 's. Moreover, once $\varphi(\sqrt{\gamma})$ and $\varphi(\sqrt{\delta})$ are fixed, $\varphi(y_1) = \pm y_i$ yields $\varphi(y_i) = \pm y_1$. So, again, we have no elements of order 8 (and, as above, they cannot all be of order 2). Since there is no privileged y -coordinate, all the elements with $\varphi(y_1) = y_i$ ($i \neq 1$) have order 4 and $\text{Gal}(K_3/K)$ is the quaternion group Q_8 with generators of order 4

$$\varphi_2 \begin{cases} y_1 \mapsto y_2 \\ \sqrt{\gamma} \mapsto \sqrt{\gamma} \end{cases}, \varphi_3 \begin{cases} y_1 \mapsto y_3 \\ \sqrt{\gamma} \mapsto -\sqrt{\gamma} \end{cases} \quad \text{and} \quad \varphi_4 \begin{cases} y_1 \mapsto y_4 \\ \sqrt{\gamma} \mapsto -\sqrt{\gamma} \end{cases}$$

and the element of order 2

$$\varphi_1 \begin{cases} y_1 \mapsto -y_1 \\ \sqrt{\gamma} \mapsto \sqrt{\gamma} \end{cases}.$$

If $d = 6$: then K_3 contains the cubic extension $K(\sqrt[3]{\Delta})$ and it must contain its Galois closure too. Hence if $\zeta_3 \in K$, we have $\text{Gal}(K_3/K) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; otherwise $K_3 = K(\sqrt[3]{\Delta}, \zeta_3)$ with $\text{Gal}(K_3/K) \simeq S_3$.

If $d = 4$: then there are three cases

- a. $K = K(\sqrt[3]{\Delta})$ and $K_3 = K(\sqrt{\delta})$, or
- b. $K = K(\sqrt[3]{\Delta})$ and $K_3 = K(\sqrt{\gamma}, y_1)$, or
- c. $K = K(\sqrt{\gamma})$ and $K_3 = K(y_1)$.

In all these cases K_3 contains a quadratic subextension K' which is either $K(\sqrt{\gamma})$ (cases **a** and **b**) or $K(\sqrt{\delta})$ (case **c**). If $\zeta_3 \notin K'$ then $K_3 = K'(\zeta_3)$ and $\text{Gal}(K_3/K') \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $\zeta_3 \in K'$, then K' is the unique quadratic subextension, $\text{Gal}(K_3/K)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and it is generated by

$$\varphi_{\mathbf{a}} \begin{cases} \sqrt{\gamma} \mapsto -\sqrt{\gamma} \\ \sqrt{\delta} \mapsto \sqrt{\delta'} \end{cases}, \quad \varphi_{\mathbf{b}} \begin{cases} \sqrt{\gamma} \mapsto -\sqrt{\gamma} \\ y_1 \mapsto y_3 \end{cases} \quad \text{or} \quad \varphi_{\mathbf{c}} \begin{cases} \sqrt{\delta} \mapsto -\sqrt{\delta} \\ y_1 \mapsto y_2 \end{cases}.$$

6 Fields $K(\mathcal{E}[4])$

This section focuses on the case $m = 4$ (we remark that the γ and δ here have no relation with the same symbols appearing in Section 5). Let K be a field, with $\text{char}(K) \neq 2, 3$, and let \mathcal{E} be an elliptic curve defined over K , with Weierstrass form $y^2 = x^3 + Ax + B$. The roots α , β and γ of $x^3 + Ax + B = 0$ are the x -coordinates of the points of order 2 of \mathcal{E} . In particular $\alpha + \beta + \gamma = 0$. The points of exact order 4 of \mathcal{E} are $\pm P_1, \pm P_2, \pm P_3, \pm P_4, \pm P_5, \pm P_6$, where

$$\begin{aligned} P_1 &= (\alpha + \sqrt{(\alpha - \beta)(\alpha - \gamma)}, (\alpha - \beta)\sqrt{\alpha - \gamma} + (\alpha - \gamma)\sqrt{\alpha - \beta}), \\ P_2 &= (\beta + \sqrt{(\beta - \alpha)(\beta - \gamma)}, (\beta - \gamma)\sqrt{\beta - \alpha} + (\beta - \alpha)\sqrt{\beta - \gamma}), \\ P_3 &= (\alpha - \sqrt{(\alpha - \beta)(\alpha - \gamma)}, (\alpha - \beta)\sqrt{\alpha - \gamma} - (\alpha - \gamma)\sqrt{\alpha - \beta}), \\ P_4 &= (\beta - \sqrt{(\beta - \alpha)(\beta - \gamma)}, (\beta - \alpha)\sqrt{\beta - \gamma} - (\beta - \gamma)\sqrt{\beta - \alpha}), \\ P_5 &= \left(\gamma + \sqrt{(\alpha - \gamma)(\beta - \gamma)}, \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \alpha}} + \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \beta}} \right), \\ P_6 &= \left(\gamma - \sqrt{(\alpha - \gamma)(\beta - \gamma)}, \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \alpha}} - \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \beta}} \right). \end{aligned}$$

We take P_1 and P_2 as basis of the 4-torsion subgroup of \mathcal{E} . With the explicit formulas for the coordinates of the 4-torsion points its easy to check that (see, for example, [6])

$$K_4 = K(\sqrt{-1}, \sqrt{\alpha - \beta}, \sqrt{\beta - \gamma}, \sqrt{\gamma - \alpha}).$$

Another quick way to find this extension is by applying Theorem 2.5.

6.1 The degree $[K_4 : K]$

By definition $K(\alpha, \beta)$ is the splitting field of $x^3 + Ax + B$, i.e., the field generated by the 2-torsion points. Hence $[K(\alpha, \beta) : K] = [K_2 : K] \leq 6$. Then $K_4 = K(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}, \sqrt{\beta - \gamma}, \sqrt{-1})$ has degree at most $16 \cdot [K(\alpha, \beta) : K] \leq 96$ which is, as expected, the cardinality of $\text{GL}_2(\mathbb{Z}/4\mathbb{Z})$. As mentioned at the beginning of Section 5.1, once we find a curve \mathcal{E} defined over \mathbb{Q} with $[\mathbb{Q}(\mathcal{E}[4]) : \mathbb{Q}] = 96$ (see Proposition 6.2 below), we know that any degree d dividing 96 is obtainable over some number field K .

Theorem 6.1. *With notations as above, put $d' := [K_2 : K]$ and $d := [K_4 : K]$. Consider the conditions*

$$\begin{aligned} \mathbf{A1.} & \sqrt{\alpha - \beta} \notin K_2, & \mathbf{A3.} & \sqrt{\beta - \gamma} \notin K_2(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}), \\ \mathbf{A2.} & \sqrt{\alpha - \gamma} \notin K_2(\sqrt{\alpha - \beta}), & \mathbf{A4.} & \sqrt{-1} \notin K(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}, \sqrt{\beta - \gamma}). \end{aligned}$$

Then the degrees are the following

d	d'	holding conditions	d	d'	holding conditions
96	6	A1, A2, A3, A4	12	3	2 among A1, A2, A3, A4
48	6	3 among A1, A2, A3, A4	8	2	2 among A1, A2, A3, A4
48	3	A1, A2, A3, A4	8	1	3 among A1, A2, A3, A4
32	2	A1, A2, A3, A4	6	6	none
24	6	2 among A1, A2, A3, A4	6	3	1 among A1, A2, A3, A4
24	3	3 among A1, A2, A3, A4	4	2	1 among A1, A2, A3, A4
16	2	3 among A1, A2, A3, A4	4	1	2 among A1, A2, A3, A4
16	1	A1, A2, A3, A4	3	3	none
12	6	1 among A1, A2, A3, A4	2	2	none
			2	1	1 among A1, A2, A3, A4

Proof. Computations are straightforward (every condition provides a degree 2 extension). \square

We show that any degree d is obtainable by providing a rather general case over \mathbb{Q} with $d = 96$. To stay coherent with our previous notations we set $\mathbb{Q}(\mathcal{E}[4]) =: \mathbb{Q}_4$ and $\mathbb{Q}(\mathcal{E}[2]) =: \mathbb{Q}_2$ (not to be confused with the 2-adic field).

Proposition 6.2. *Assume that $x^3 + Ax + B \in \mathbb{Q}[x]$ is irreducible, that $\Delta = -16(27B^2 + 4A^3)$ is positive and not a square in \mathbb{Q} and that α, β and γ are pairwise distinct real numbers. Then $[\mathbb{Q}_4 : \mathbb{Q}] = 96$.*

Proof. Put $\delta = -3\alpha^2 - 4A$ and note that, once α is fixed the other two roots are $\frac{-\alpha \pm \sqrt{\delta}}{2}$. By renaming the three roots (if necessary), we may assume that $\alpha > \beta > \gamma$, so that all the generators except $\sqrt{-1}$ are real and

$$\begin{aligned} [\mathbb{Q}_4 : \mathbb{Q}] &= 2[\mathbb{Q}(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}, \sqrt{\beta - \gamma}) : \mathbb{Q}] \\ &= 2[\mathbb{Q}\left(\sqrt{\frac{3\alpha + \sqrt{\delta}}{2}}, \sqrt{\frac{3\alpha - \sqrt{\delta}}{2}}, \sqrt[4]{\delta}\right) : \mathbb{Q}]. \end{aligned} \tag{3}$$

By the choice of α , we have that $A < 0$ and the polynomial $x^3 + Ax + B$ has a minimum in $x = \sqrt{-\frac{A}{3}}$. Hence $\alpha > \sqrt{-\frac{A}{3}}$ and in particular $3\alpha^2 + A > 0$.

By the hypotheses, we have that $[\mathbb{Q}_2 : \mathbb{Q}] = [\mathbb{Q}(\alpha, \sqrt{\delta}) : \mathbb{Q}] = 6$ and $\delta > 0$ is not a square in $\mathbb{Q}(\alpha)$. Obviously $[\mathbb{Q}_2(\sqrt[4]{\delta}) : \mathbb{Q}_2] = 2$; moreover $\frac{3\alpha + \sqrt{\delta}}{2}$ is a square in \mathbb{Q}_2 if and only if $\frac{3\alpha - \sqrt{\delta}}{2}$ has the same property. Assume $\frac{3\alpha + \sqrt{\delta}}{2} \in (\mathbb{Q}_2^*)^2$, i.e., $\frac{3\alpha + \sqrt{\delta}}{2} = (a + b\sqrt{\delta})^2$, for some $a, b \in \mathbb{Q}_2$. Then

$$\begin{cases} a^2 + b^2\delta = \frac{3\alpha}{2} \\ 2ab = \frac{1}{2} \end{cases} \implies \begin{cases} a^2 + \frac{\delta}{16a^2} = \frac{3\alpha}{2} \\ b = \frac{1}{4a} \end{cases},$$

leading to

$$a^2 = \frac{12\alpha \pm \sqrt{144\alpha^2 - 16\delta}}{16} = \frac{3\alpha \pm \sqrt{9\alpha^2 - \delta}}{4} \in \mathbb{Q}(\alpha) .$$

Hence $9\alpha^2 - \delta = 12\alpha^2 + 4A$ must be a square in $\mathbb{Q}(\alpha)$, i.e., $3\alpha^2 + A \in (\mathbb{Q}(\alpha)^*)^2$. Let N denote the norm map from $\mathbb{Q}(\alpha)$ to \mathbb{Q} . Then $N(3\alpha^2 + A) = 27B^2 + 4A^3$ is not a square in \mathbb{Q} by hypothesis and this contradicts $3\alpha^2 + A \in (\mathbb{Q}(\alpha)^*)^2$. Therefore

$$[\mathbb{Q}_2 \left(\sqrt{\frac{3\alpha + \sqrt{\delta}}{2}} \right) : \mathbb{Q}_2] = [\mathbb{Q}_2 \left(\sqrt{\frac{3\alpha - \sqrt{\delta}}{2}} \right) : \mathbb{Q}_2] = 2$$

and we have to prove that the three quadratic extensions of \mathbb{Q}_2 we found are independent.

The elements $\sqrt{\frac{3\alpha + \sqrt{\delta}}{2}}$ and $\sqrt{\frac{3\alpha - \sqrt{\delta}}{2}}$ generate the same quadratic extension over \mathbb{Q}_2 if and only if

$$\frac{3\alpha + \sqrt{\delta}}{2} \cdot \frac{2}{3\alpha - \sqrt{\delta}} = \frac{9\alpha^2 - \delta}{(3\alpha - \sqrt{\delta})^2} \in (\mathbb{Q}_2^*)^2 ,$$

i.e., if and only if $3\alpha^2 + A \in (\mathbb{Q}_2^*)^2$. We have already seen that $3\alpha^2 + A \notin (\mathbb{Q}(\alpha)^*)^2$, so we must have $3\alpha^2 + A = (a + b\sqrt{\delta})^2$ with $a, b \in \mathbb{Q}(\alpha)$ and $b \neq 0$. A little computation gives

$$b^2 = -\frac{3\alpha^2 + A}{3\alpha^2 + 4A} \in (\mathbb{Q}(\alpha)^*)^2 ,$$

but

$$N \left(-\frac{3\alpha^2 + A}{3\alpha^2 + 4A} \right) = -1 \notin (\mathbb{Q}^*)^2$$

and this is a contradiction. Hence

$$[\mathbb{Q}_2 \left(\sqrt{\frac{3\alpha + \sqrt{\delta}}{2}}, \sqrt{\frac{3\alpha - \sqrt{\delta}}{2}} \right) : \mathbb{Q}_2] = 4 .$$

Now $\sqrt[4]{\delta}$ and $\sqrt{\frac{3\alpha \pm \sqrt{\delta}}{2}}$ generate the same quadratic extension of \mathbb{Q}_2 if and only if

$$\frac{3\alpha \pm \sqrt{\delta}}{2} \cdot \frac{1}{\sqrt{\delta}} = \frac{6\alpha\sqrt{\delta} \pm 2\delta}{4\delta} \in (\mathbb{Q}_2^*)^2$$

i.e., if and only if $6\alpha\sqrt{\delta} \pm 2\delta = (a + b\sqrt{\delta})^2$ for some $a, b \in \mathbb{Q}(\alpha)$. This leads to

1. $a^2 + b^2\delta = 2\delta$ and $2ab = 6\alpha$: solving for a we get

$$a^2 = \delta \pm \sqrt{\delta^2 - 9\alpha^2\delta} \in \mathbb{Q}(\alpha) .$$

Hence

$$\delta^2 - 9\alpha^2\delta = (-3\alpha^2 - 4A)(-12\alpha^2 - 4A) \in (\mathbb{Q}(\alpha)^*)^2$$

i.e., $(3\alpha^2 + 4A)(3\alpha^2 + A) \in (\mathbb{Q}(\alpha)^*)^2$. But by hypothesis $3\alpha^2 + 4A = -\delta < 0$ and we recall that $3\alpha^2 + A > 0$; thus $(3\alpha^2 + 4A)(3\alpha^2 + A) < 0$ cannot be a square in the real field $\mathbb{Q}(\alpha)$.

2. $a^2 + b^2\delta = -2\delta$ and $2ab = 6\alpha$: this is impossible because $a^2 + b^2\delta > 0$, while $-2\delta < 0$.

Then

$$[\mathbb{Q}_2 \left(\sqrt[4]{\delta}, \sqrt{\frac{3\alpha + \sqrt{\delta}}{2}} \right) : \mathbb{Q}_2] = [\mathbb{Q}_2 \left(\sqrt[4]{\delta}, \sqrt{\frac{3\alpha - \sqrt{\delta}}{2}} \right) : \mathbb{Q}_2] = 4 .$$

With similar computations one checks that the extension generated by $\sqrt[4]{\delta}$ is also independent from the third quadratic extension contained in $\mathbb{Q}_2 \left(\sqrt{\frac{3\alpha + \sqrt{\delta}}{2}}, \sqrt{\frac{3\alpha - \sqrt{\delta}}{2}} \right)$, which is $\mathbb{Q}_2(\sqrt{3\alpha^2 + A})$. Hence

$$[\mathbb{Q}_2 \left(\sqrt{\frac{3\alpha + \sqrt{\delta}}{2}}, \sqrt{\frac{3\alpha - \sqrt{\delta}}{2}}, \sqrt[4]{\delta} \right) : \mathbb{Q}] = 48$$

and, by (3), we have $[\mathbb{Q}_4 : \mathbb{Q}] = 96$. □

With reducible polynomials $x^3 + Ax + B$ we can easily obtain examples of smaller degrees, in particular when $A = 0$ or $B = 0$ (obviously, since $\sqrt{-1} \in \mathbb{Q}_4$, we cannot obtain extension of degree 1 or 3 over \mathbb{Q}).

Example 6.3. The curve

$$y^2 = x^3 - \frac{481}{3}x + \frac{9658}{27} = \left(x - \frac{34}{3}\right) \left(x - \frac{7}{3}\right) \left(x + \frac{41}{3}\right)$$

provides $\sqrt{\alpha - \beta} = 3$, $\sqrt{\alpha - \gamma} = 5$ and $\sqrt{\beta - \gamma} = 4$. Then $\mathbb{Q}_4 = \mathbb{Q}(\sqrt{-1})$ has degree 2 over \mathbb{Q} . The curve

$$y^2 = x^3 - 22x - 15 = (x - 5)(x^2 + 5x + 3)$$

yields

$$\mathbb{Q}_2 = \mathbb{Q}(\sqrt{13}) \quad \text{and} \quad \mathbb{Q}_4 = \mathbb{Q} \left(\sqrt{\frac{5 + \sqrt{13}}{2}}, \sqrt{\frac{5 - \sqrt{13}}{2}}, \sqrt[4]{5}, \sqrt{-1} \right)$$

which has degree 32 over \mathbb{Q} .

Proposition 6.4. *If $A = 0$, then $\mathbb{Q}_4 = \mathbb{Q}(\zeta_{12}, \sqrt{\sqrt[3]{B}(1 - \zeta_3)})$ and*

$$[\mathbb{Q}_4 : \mathbb{Q}] = \begin{cases} 8 & \text{if } B \in (\mathbb{Q}^*)^3, \\ 24 & \text{otherwise.} \end{cases}$$

If $B = 0$, then $\mathbb{Q}_4 = \mathbb{Q}(\sqrt{2}, \sqrt{-1}, \sqrt[4]{-A})$ and

$$[\mathbb{Q}_4 : \mathbb{Q}] = \begin{cases} 16 & \text{if } A \neq \pm 2a^2, \pm a^2 \text{ with } a \in \mathbb{Q}, \\ 8 & \text{if } A = \pm 2a^2 \text{ with } a \in \mathbb{Q}, \\ 4 & \text{if } A = a^4, \pm 4a^4 \text{ with } a \in \mathbb{Q}, \\ 8 & \text{otherwise.} \end{cases}$$

Proof. For $A = 0$ just take $\alpha = \sqrt[3]{B}$, $\beta = \zeta_3 \sqrt[3]{B}$ and $\gamma = \zeta_3^2 \sqrt[3]{B}$ to get

$$\mathbb{Q}_4 = \mathbb{Q} \left(\zeta_3, \sqrt{-1}, \sqrt{\sqrt[3]{B}(1 - \zeta_3)}, \sqrt{\sqrt[3]{B}(1 - \zeta_3^2)}, \sqrt{\sqrt[3]{B}(\zeta_3 - \zeta_3^2)} \right) .$$

Obviously $\mathbb{Q}(\zeta_3, \sqrt{-1}) = \mathbb{Q}(\zeta_{12})$, moreover, the elements $\sqrt[3]{B(1 - \zeta_3)}$, $\sqrt[3]{B(1 - \zeta_3^2)}$ and $\sqrt[3]{B(\zeta_3 - \zeta_3^2)}$ generate the same extension of $\mathbb{Q}(\zeta_{12})$. Therefore

$$\mathbb{Q}_4 = \mathbb{Q}\left(\zeta_{12}, \sqrt[3]{B(1 - \zeta_3)}\right)$$

and the first statement follows.

For $B = 0$ let $\alpha = 0$, $\beta = \sqrt{-A}$ and $\gamma = -\beta$ to get $\mathbb{Q}_4 = \mathbb{Q}(\sqrt[4]{-A}, \sqrt{2}, \sqrt{-1})$. The unique quadratic subfield of $\mathbb{Q}(\sqrt[4]{-A})$ is $\mathbb{Q}(\sqrt{-A})$, hence, if $\mathbb{Q}(\sqrt{-A}) \neq \mathbb{Q}(\sqrt{\pm 2})$, $\mathbb{Q}(\sqrt{-1})$, \mathbb{Q} , i.e., if $A \neq \pm 2a^2, \pm a^2$ for some $a \in \mathbb{Q}$, we have $[\mathbb{Q}_4 : \mathbb{Q}] = 16$. The remaining cases are straightforward. \square

6.2 Galois groups

One can find descriptions for $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ in [1, Section 5.1] or [7, Section 3]: the most suitable for our goals is the exact sequence coming from the canonical projection $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, whose kernel we denote by H_2^4 . Obviously

$$H_2^4 = \left\{ \begin{pmatrix} 1+2a & 2b \\ 2c & 1+2d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \right\}$$

and it is easy to check that it is an abelian group of order 16 and exponent 2, i.e., isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. By sending the row (1 1) to (3 3) and leaving rows (1 0) and (0 1) fixed, we see that there exists a section $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ which splits the sequence

$$H_2^4 \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

as a semi-direct product. For any K , we have a commutative diagram

$$\begin{array}{ccccc} H_2^4 & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) & \twoheadrightarrow & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(K_4/K_2) & \hookrightarrow & \mathrm{Gal}(K_4/K) & \twoheadrightarrow & \mathrm{Gal}(K_2/K) \end{array}$$

The structure of $\mathrm{Gal}(K_4/K)$ can be derived from the lower sequence (which splits as well), checking the conditions of Theorem 6.1 to compute d' (which identifies $\mathrm{Gal}(K_2/K)$ as one among Id , $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ or S_3) and the $i \in \{0, \dots, 4\}$ for which $\mathrm{Gal}(K_4/K_2) \simeq (\mathbb{Z}/2\mathbb{Z})^i$.

References

- [1] C. ADELMANN, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics **1761**, Springer-Verlag, Berlin, 2001.
- [2] A. BANDINI, Three-descent and the Birch and Swinnerton-Dyer conjecture, *Rocky Mount. J. of Math.* **34** (2004), 13–27.
- [3] A. BANDINI, 3-Selmer groups for curves $y^2 = x^3 + a$, *Czechoslovak Math. J.* **58** (2008), 429–445.
- [4] A. BANDINI AND L. PALADINO, Number fields generated by the 3-torsion points of an elliptic curve, *Monatsh. Math.* **168**, no. 2 (2012), 157–181.

- [5] R. DVORNICICH AND U. ZANNIER, Local-global divisibility of rational points in some commutative algebraic groups, *Bull. Soc. Math. France* **129**, no. 3 (2001), 317–338.
- [6] R. DVORNICICH R. AND U. ZANNIER, An analogue for elliptic curves of the Grunwald-Wang example, *C. R. Acad. Sci. Paris, Ser. I* **338** (2004), 47–50.
- [7] C. HOLDEN, Mod 4 Galois representations and elliptic curves, *Proc. Amer. Math. Soc.* **136**, no. 1 (2008), 31–39.
- [8] N.M. KATZ - B. MAZUR, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies **108**, Princeton Univ. Press, Princeton, 1985.
- [9] E. LARSON AND D. VAINTROB, On the surjectivity of Galois representations associated to elliptic curves over number fields, *Bull. Lond. Math. Soc.* **46**, no. 1 (2014), 197–209.
- [10] L. PALADINO, Local-global divisibility by 4 in elliptic curves defined over \mathbb{Q} , *Annali di Matematica Pura e Applicata* **189**, no. 1 (2010), 17–23.
- [11] L. PALADINO, Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9, *J. Théor. Nombres Bordeaux* **22** (2010), no. 1, 138–160.
- [12] J. REYNOLDS, On the pre-image of a point under an isogeny and Siegel’s theorem, *New York J. Math.* **17** (2011), 163–172.
- [13] E.F. SCHAEFER AND M. STOLL, How to do a p -descent on an elliptic curve, *Trans. Amer. Math. Soc.* **356** (2004), 1209–1231.
- [14] J.-P. SERRE, Propriétés Galoisiennes des points d’ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
- [15] J.-P. SERRE, Quelques applications du théorème de densité de Chebotarev, *Ist. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401.
- [16] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, 1971.
- [17] J.H. SILVERMAN, *The arithmetic of elliptic curves, 2-nd edition*, **GTM 106** Springer-Verlag, New York, 2009.
- [18] J.H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, **GTM 151** Springer-Verlag, New York, 1994.